AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
INFORMATION STORED IN THE SERVER THAT IS ASSOCIATED WITH IP ADDRESS 104.232.35[.]104 AND IS LOCATED AT PREMISES CONTROLLED BY NET3 INC

Case No. 1:17-SW-19

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
See Attachment A

located in the Western District of New York, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1029, 1030, 1343, 2511, and 2512	Fraud and related activity in connection with access devices and computers; fraud by wire, radio, or television; manufacture, distribution, possession, and use of electronic communication intercepting devices.

The application is based on these facts:
See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:
Whitney Russell, AUSA

Applicant's signature

Cole Ashcraft, Special Agent, USPS OIG
Printed name and title

Sworn to before me and signed in my presence.

Date: 1/19/17

/s/
Theresa Carroll Buchanan
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia

The Honorable Theresa C. Buchanan, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN THE MATTER OF THE SEARCH OF INFORMATION STORED IN THE SERVER THAT IS ASSOCIATED WITH IP ADDRESS 104.232.35[.]104 AND IS LOCATED AT PREMISES CONTROLLED BY NET3 INC	Case No. 1:17-SW-19 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Cole Ashcraft, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Net3 Inc. (Net3) to disclose to the government records and other information in its possession, as further specified in the Attachments to this affidavit.

2. I am a Special Agent with the United States Postal Service (Postal Service) Office of Inspector General (USPS OIG), and have been since 2013. I have received formal training in the investigation of computer crimes, including network intrusions, from the Defense Cyber Investigations Training Academy in Linthicum, MD and the U.S. Department of Homeland Security in Arlington, VA. I have a bachelor's degree in Computer Science and Geography and a master's degree in Cyber Security in Computer Science, both from The George Washington University in Washington, DC. I have investigated or assisted in the investigation of a number of cases involving fraudulent activity in connection with computers. I am currently assigned to the Postal Service OIG's Computer Crimes Unit and investigate violations of federal laws regarding property in the custody of the Postal Service, property of the Postal Service, the use of the mails,

and other postal offenses. I have received extensive specialized training in these fields. I have been a sworn law enforcement officer during all times herein.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1029, 1030, 1343, 2511, and 2512 have been committed by unknown actors. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B.

5. The TARGET SERVER is a server associated with the Internet Protocol address 104.232.35[.]104. The TARGET SERVER is located at premises located in Western District of New York owned, maintained, controlled, or operated by Net3 Inc., a company that receives correspondence at 170 - 422 Richards St, Vancouver, BC V6B 2Z4, Canada. As detailed later in this affidavit, Net3 is a provider of electronic communication or remote computing services operating in the United States, despite its Canadian address.

PROBABLE CAUSE

The Nemesis Intrusions

6. Victim 1 is a payment gateway. As a payment gateway, Victim 1 receives data regarding credit card transactions from client merchants across the United States, including merchants in the Eastern District of Virginia, and transmits those transactions to multiple

payment processors for processing and settlement. Victim 1's computers are protected computers within the definition at 18 U.S.C. § 1030(e)(2)(B), as they are computers used in interstate commerce.

7. From October 26, 2009, to September 24, 2014, Victim 1 experienced a sophisticated malicious intrusion into its servers.

8. Forensic examination of these servers indicated unknown actors obtained and maintained unauthorized access by installing malicious software to maintain their access and surreptitiously intercepted electronic communications between the compromised servers and various credit card payment processors.

9. The unknown actors relied heavily on a custom piece of malicious software, named "Nemesis" by its creators, to maintain access and intercept Victim 1's electronic communications. Nemesis appears to be designed specifically for surreptitious interception of electronic communications, rather than to perform any legitimate network administration functions. For example, Nemesis obfuscates intercepted electronic communications using either a primitive cryptographic routine or a modern cryptographic algorithm. This obfuscation routine prevents someone inspecting files containing intercepted communications from readily ascertaining the contents of the files, enabling them to be hidden in plain sight on victim servers. This feature is indicative of malicious use because hiding intercepted communications in plain sight on the victim servers, as was done at Victim 1 and would be in a typical use case for Nemesis, would be entirely unnecessary if an authorized party is overtly monitoring communications. Additionally, some Nemesis variants have interception capabilities designed to exclusively target electronic communications on specific portions of a specific victim's network; prior to notification by the government, the victim was unaware of the existence or use of such

software. As further proof that Nemesis is designed for surreptitious use, the obfuscation routine also prevents legitimate network traffic analysis tools from reading the captured communications. That Nemesis and its communication-intercepting abilities evaded detection on Victim 1's network for almost five years is further proof of its capabilities and design for surreptitious operation. As a result, 18 U.S.C. §§ 2511 and 2512 proscribe the manufacture, distribution, possession, and use the Nemesis malware.

10. The forensic analysis of Victim 1's servers also indicated that the unknown actors used Nemesis to commit violations of various United States laws. For example, these actors used Nemesis to intercept electronic communications containing authorization and settlement transactions destined for multiple payment processors, including the credit card numbers involved in the transactions and other card and cardholder data; these items constitute unauthorized access devices within the definition at 18 U.S.C. § 1029(e)(3). The unknown actors then transferred these unlawfully intercepted electronic communications to servers they controlled outside Victim 1's network. Certain of the card numbers and associated data were subsequently used for fraudulent purchases, including card numbers for numerous Postal Service credit cards. These transfers and the command and control traffic used to orchestrate this intrusion constitute signals transmitted by wire in interstate commerce in furtherance of a scheme to defraud, in violation of 18 U.S.C. § 1343. During the last six weeks of the intrusion, these intercepted communications included more than 710,000 unencrypted payment card numbers and associated data; the possession of these card numbers constitutes a violation of 18 U.S.C. § 1029(a)(3). Forensic artifacts indicate the actors likely intercepted electronic communications containing credit card data during the entire period from November 2009 to September 2014, impacting more than two million cards.

11. Yellow Cab of Prince William County and Regency Taxi, businesses operating in the Eastern District of Virginia, used Victim 1's services to process credit cards during the period Victim 1's computers were compromised by Nemesis and other malicious software. As a result of this compromise, the unknown actors obtained and fraudulently used the credit card numbers of customers of both businesses.

12. Victim 2 is a business that operates a large number of automated teller machines (ATMS) in the Americas and Europe. By early 2010, the same unknown subjects gained and maintained access to Victim 2's network using the Nemesis malware and command and control infrastructure that overlapped with or was linked to infrastructure used in the intrusion at Victim 1. According to Victim 2's information security personnel, the intrusion continued through at least early August 2015.

13. Victim 2's information security personnel, with assistance from federal law enforcement, have determined that Nemesis was used to intercept network traffic containing ATM transactions and that, beginning in mid-June 2015, the intruders used a server at the domain coreduck[.]net to maintain unauthorized access to and control their compromised computer systems. Based on knowledge of how the unknown subjects use Nemesis and historical patterns of activity, investigators believe the unknown subjects likely exfiltrated information from Victim 2 to the server at coreduck[.]net.

14. A Nemesis version installed on many of Victim 2's computers creates encrypted debug log. These logs automatically document, in detail, actions the unknown subjects took using the Nemesis malware. At Victim 2, these logs show the unknown subjects configured compromised computers at Victim 2 to open a reverse shell – meaning a compromised computer

opens a network connection to the unknown subject's computer over which they can execute arbitrary commands on the compromised computer – to a server at the domain dipwitch[.]com.

The Target Server

15. By early November 2015, resolution for both domains – dipwitch[.]com and coreduck[.]net – had been changed so that both domains resolved to the IP address 69.175.121[.]226 (VICTIM SERVER 1). At that time Victim 3, a legitimate business unrelated to Victim 1 and 2, controlled VICTIM SERVER 1. Investigators searched VICTIM SERVER 1 pursuant to search warrants from this Court and consent from the server's owner and operator. Forensic examination of VICTIM SERVER 1 indicated that shortly before the DNS records for dipwitch[.]com and coreduck[.]net were changed to point to VICTIM SERVER 1, the unknown actors gained unauthorized access to VICTIM SERVER 1 by exploiting a vulnerability in a web page it hosted; the DNS changes after exploitation likely indicate subsequent use of VICTIM SERVER 1 in the Nemesis intrusions. This vulnerability allowed the actors to execute arbitrary commands on the server, without authentication. Using this vulnerability, they executed a series of obfuscated commands to place their tools on VICTIM SERVER 1 and run them. One of the commands executed as part of this process appears to have configured VICTIM SERVER 1 to open a connection to the TARGET SERVER over which commands could be executed or files transferred. Shortly thereafter, Nemesis malware that specifically targets Victim 2 was installed VICTIM SERVER 1 and used to probe a server belonging to Victim 2. These actions occurred from a small range of IP addresses in Russia that have previously been observed purchasing and connection to command and control infrastructure for these intrusions.

16. In my training and experience, the context in which the TARGET SERVER appears on VICTIM SERVER 1 likely indicates it was used to bootstrap the compromise of

VICTIM SERVER 1, in order to facilitate the continued targeting of Victim 2, and is under the unknown actor's control. If this is the case, the TARGET SERVER is likely to contain evidence of a crime and be itself an instrumentality of a crime.

Jurisdiction of this Court to issue the requested warrant

17. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

18. Net3, despite being headquartered in Canada, is a U.S. provider of electronic communication and remote computing services for the purposes of the Electronic Communications Privacy Act (18 U.S.C. § 2701 *et seq.*), and therefore subject to the jurisdiction of this Court, by virtue of having servers physically located in the United States and an employee in the United States who accepts service of legal process.

19. The IP address for the TARGET SERVER is assigned to ColoCrossing, a hosting and colocation provider located at 325 Deleware Ave #300, Buffalo, NY 14202. In response to an order from this Court, ColoCrossing advised they have assigned this IP address to Net3, who resells ColoCrossing's services to other customers; this is a common business arrangement in the information technology sector. ColoCrossing's servers – to which Net3 has re-sold access – are physically located in the United States, specifically, in Buffalo, NY in the Western District of New York. A person Net3 identifies as "Thomas H." accepts service of legal process on behalf of Net3. Net3's Chief Technology Officer confirmed to the Royal Canadian Mounted Police that "Thomas H." is an employee of the company and a natural person located in the United States.

Facts about Net3 and hosting companies

20. A server is a computer, connected to the Internet, that provides services to other computers. A web server, for example, sends web pages to a user's computer when a user requests those web pages. Customers can connect from their own computers to the server computers across the Internet. This connection can occur in several ways. In some situations, it is possible for a customer to upload files using a special web site interface offered by a web hosting company. It is frequently also possible for the customer to directly access the server computer through the Secure Shell ("SSH") or Telnet protocols. These protocols allow remote users to type commands to the server. The SSH protocol can also be used to copy files to the server. Customers can also upload files through a different protocol, known as File Transfer Protocol ("FTP"). Servers often maintain logs of SSH, Telnet, and FTP connections, showing the dates and times of the connections, the method of connecting, and the Internet Protocol addresses ("IP addresses") of the remote users' computers (IP addresses are used to identify computers connected to the Internet). Servers also commonly log the port number associated with the connection. Port numbers assist computers in determining how to interpret incoming and outgoing data. For example, SSH, Telnet, and FTP are generally assigned to different ports.

21. Hosting companies, such as Net3, maintain, or lease from others, server computers connected to the Internet. Through a variety of possible arrangements, hosting companies sell to customers the right to use their server computers. In some arrangements, a single customer has exclusive control over an entire server. In other arrangements, multiple independent customers share the use of a single server. In these shared-hosting arrangements, individual customers can each upload their own data and programs and can edit and delete their own data, but often have limited access to other users' data.

22. The warrant I apply for seeks the entire TARGET SERVER as property to be seized. While, given Net3's service offerings, it is likely the TARGET SERVER is allocated for the sole use of a single customer, this is not definitively known as this time. Even so, searching and seizing the entire TARGET SERVER is justified for several reasons. For instance, certain versions of the Nemesis malware store their executable code and other data in unusual places, such as the ordinarily unused space on hard drives between the portions of the drive allocated for use by a particular partition or operating system. Data in these spaces can only be discovered through an exhaustive search of the entire TARGET SERVER.

23. Pursuant to a warrant from this Court, I previously searched another command and control server with which Victim 2 was also communicating. This server also had the Nemesis malware installed on it, likely because the Nemesis malware can be used to connect to other instances of the Nemesis malware. Given that two command and control domains for Nemesis malware now resolve to the TARGET SERVER, it is likely the TARGET SERVER is being used for the same or similar purposes and will have the same or similar configuration. The Nemesis malware, by its nature, subverts separation that might be imposed by a hosting provider on a shared server and transforms the server into an instrumentality for the criminal conduct described above. Finally, given that the unknown suspects have demonstrated technical prowess in and a propensity for gaining unauthorized access to even well-secured computer systems, it seems naïve to assume they would confine their activities exclusively to the portion of a shared computer system allocated for their use. Consequently, there is probable cause to believe that all data recorded on the computer is potentially evidence of a crime or of crimes, either because it directly reflects criminal activity or because it is evidence of how the TARGET SERVER was configured to behave and act as an instrumentality of crime.

THE NATURE OF EXECUTION

24. Net3 has electronic access to the TARGET SERVER. Moreover, Net3 provides Internet connectivity to the servers at its facility. Thus, I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Net3 to disclose to the government records. Specifically, Net3 will be compelled to disclose copies of the records and other information particularly described in Section I of Attachment B. Government agents will serve this warrant on Net3, perhaps delivering the warrant in person. It is possible that Net3 will request the assistance of the government in making the necessary copies; if asked for such assistance, the government will provide it.

25. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B. The examination may require techniques, including but not limited to computer-assisted scans, that might expose many parts of the data to human inspection in order to determine whether it is evidence described by the warrant.

26. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. However, I expect that government agents will offer to assist Net3 in the task of complying with this warrant, including by making the necessary copies of data. Net3 will be free to decline that assistance, but is compelled to disclose the data regardless.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

27. As described above and in the Attachments, this application seeks permission to obtain a copy of the entire TARGET SERVER and to examine the TARGET SERVER for

records that might be recorded upon it. I submit that there is probable cause to believe those records will be stored on the TARGET SERVER, both for the reasons given above and also for at least the following reasons:

28. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been written to a storage medium, such as a hard drive in the TARGET SERVER. Electronic files written to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can sometimes be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file often does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

29. Therefore, deleted files, or remnants of deleted files, may reside in free space or unallocated space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

30. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

31. *Forensic evidence.* As further described in the Attachments, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the TARGET SERVER was used, the purpose of its use, who used it, and when. There is probable cause to believe that examining the TARGET SERVER will reveal this forensic electronic evidence because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file. Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates)

may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium

for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime.

32. *Necessity of compelling the disclosure of all information stored on the TARGET SERVER.* It is necessary to compel Net3 to disclose the entire TARGET SERVER because:

a. Tasking Net3 with identifying all the evidence in Part II of Attachment B would be impossible. Net3 is not necessarily aware of the contents of the TARGET SERVER, and does not have the capability to isolate data based on subject-matter criteria.

b. Even if Net3 were to invite government agents onto the premises of Net3 to conduct a search, analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

c. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available

makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data.

CONCLUSION

33. Based on the forgoing, I submit that probable cause has been established sufficient for the Court to issue the proposed search warrant.

Respectfully submitted,

Cole S. Ashcraft
Special Agent
United States Postal Service
Office of Inspector General

Subscribed and sworn to before me
on 1/19/17:

/s/
Theresa Carroll Buchanan
United States Magistrate Judge

HON. THERESA C. BUCHANAN
UNITED STATES MAGISTRATE JUDGE